# Avtal om gemensamt personuppgiftsansvar

# Parter

1. Uppsala universitet, [institution], org.nr. 202100-2932, [adress] (nedan ”**UU**”);

och

1. [Namn], org.nr. […], [adress] (nedan ”[**…**]”)

har denna dag ingått följande Avtal om gemensamt personuppgiftsansvar för personuppgiftsbehandling (”**Avtalet**”).

 UU och […] benämns nedan gemensamt ”Parterna” och individuellt ”Part”.

# Bakgrund och syfte

Parterna har ingått ett avtal rörande [xxxx] (”**Huvudavtalet**”). För att uppfylla sina åtaganden enligt Huvudavtalet kommer Parterna att behandla personuppgifter. Detta Avtal ska säkerställa att de Personuppgifter som enligt Huvudavtalet ska behandlas hanteras i enlighet med de krav som följer av Dataskyddsförordningen, annan gällande lagstiftning och etablerad standard samt att Personuppgifterna inte blir tillgängliga för obehöriga.

Parterna är överens om att båda Parter är gemensamt Personuppgiftsansvariga och att Avtalet täcker samtliga behandlingar av Personuppgifter som sker inom ramen för Huvudavtalet.

# Definitioner

Detta Avtal har motsvarande definitioner som återfinns i artikel 4 i Dataskyddsförordningen, vilket bland annat innebär följande.

Med **Behandling** (eller **Behandla**) avses en åtgärd eller kombination av åtgärder beträffande Personuppgifter eller uppsättning av Personuppgifter, oberoende av om de utförs automatiserat eller inte, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämnande genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring.

Med **Dataskyddsförordningen** avses Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på Behandling av Personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning) (EUT 119, 4.5.2016, s. 1).

Med **Känsliga Personuppgifter** avses Personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening och Behandling av genetiska uppgifter, biometriska uppgifter för att entydigt identifiera en fysisk person, uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning.

Med **Personuppgifter** avses varje upplysning som avser en identifierad eller identifierbar fysisk person, varvid en identifierbar fysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringsuppgift eller online-identifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet.

Med **Personuppgiftsansvarig** avses en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensam eller tillsammans med andra bestämmer ändamålen och medlen för Behandling av Personuppgifter; om ändamålen och medlen för Behandling bestäms av unionsrätten eller medlemsstaternas nationella rätt kan den Personuppgiftsansvarige eller de särskilda kriterierna för hur denne ska utses föreskrivas i unionsrätten eller i medlemsstaternas nationella rätt.

Med **Personuppgiftsbiträde** avses en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som Behandlar Personuppgifter för den Personuppgiftsansvariges räkning.

Med **Personuppgiftsincident** avses en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust, eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de Personuppgifter som överförts, lagrats eller på annat sätt Behandlats.

Med **Registrerad** avses den person som Personuppgiften avser.

# Avtalets handlingar

Detta Avtal består av detta dokument, inklusive **Bilaga 1** och **Bilaga 2**.

# Parternas allmänna åtaganden

* 1. Parterna ansvarar för att den Behandling av Personuppgifter som respektive Part genomför inom ramen för detta Avtal är förenlig med Dataskyddsförordningen och annan tillämplig lagstiftning.
	2. Parterna ansvarar var och en för sig samt gemensamt att det finns en laglig grund för Behandlingen och att Personuppgifterna inte Behandlas på ett sätt som går utöver Behandlingens ändamål.
	3. Om en Behandling sannolikt leder till en hög risk för de Registrerade ansvarar Parterna för att genomföra en konsekvensbedömning i enlighet med artikel 35 Dataskyddsförordningen.
	4. Parterna ska begränsa tillgängligheten till Personuppgifterna till endast den personal vid Parten som har behov av Personuppgifterna för att uppfylla sina förpliktelser i enlighet med Huvudavtalet och detta Avtal.
	5. Parterna ska vidta lämpliga tekniska och organisatoriska skyddsåtgärder för att säkerställa att de Registrerades rättigheter skyddas. Parterna ansvarar för att Behandlingen och dess skyddsåtgärder kontinuerligt utvärderas och uppdateras. Parterna ansvarar för att Behandlingen sker enligt den säkerhetsstandard som framgår av Bilaga 2
	6. Den Part som samlar in Personuppgifterna ansvarar för att de Registrerade är informerade om Behandlingen. Denna skyldighet innebär även att generell information om innehållet i detta Avtal ska finnas med i informationen till de Registrerade.
	7. Parterna ska vidta nödvändiga åtgärder för att tillvarata de Registrerades intressen och de rättigheter som följer av Dataskyddsförordningen och annan tillämplig lagstiftning.

# Personuppgiftsbiträde

6.1 Part äger anlita Personuppgiftsbiträde för Behandling av Personuppgifter inom ramen för detta Avtal. När Personuppgifter behandlas av ett Personuppgiftsbiträde ska hanteringen regleras genom ett personuppgifts-biträdesavtal i enlighet med artikel 28 i Dataskyddsförordningen.

6.2 Part som anlitar ett Personuppgiftsbiträde ska informera den andra Parten därom samt ansvarar gentemot den andra Parten för överföring till/från samt Personuppgiftbiträdets Behandling av Personuppgifterna.

# Överföring av Personuppgifter till tredje land

7.1 En överföring till tredje land förutsätter att de krav och åtgärder som följer av Dataskyddsförordningen är uppfyllda.

7.2 Parterna är överens om att en överföring av Personuppgifter till tredje land förutsätter samtliga Parters skriftliga medgivande.

# Personuppgiftsincident

8.1 Parterna ansvarar för att omedelbart vidta rimliga åtgärder för begränsande av skadeverkningar till följd av en Personuppgiftsincident.

8.2 Parterna ansvarar för att skyndsamt informera varandra om en Personuppgiftsincident. Informationen ska åtminstone innehålla:

a) Personuppgiftsincidentens art, inbegripet, om så är möjligt, de kategorier av och det ungefärliga antalet registrerade som berörs samt de kategorier av och det ungefärliga antalet personuppgiftsposter som berörs,

b) Namnet på och kontaktuppgifterna för Dataskyddsombudet eller andra kontaktpunkter där mer information kan erhållas,

c) De sannolika konsekvenserna av Personuppgiftsincidenten, och

d) De åtgärder som vidtagits eller föreslagits för att åtgärda Personuppgiftsincidenten, inbegripet, när så är lämpligt, åtgärder för att mildra dess potentiella negativa effekter.

8.3 Parterna är överens om att, vid behov, bistå varandra med rimligt stöd för att hanteringen av Personuppgiftsincidenter är förenlig med Dataskyddsförordningen och annan tillämplig lagstiftning.

8.4 Parterna har ett gemensamt ansvar att anmäla Personuppgiftsincident till tillsynsmyndigheten och, om så krävs/nödvändigt, informera berörda Registrerade. Parterna är överens om att sådan anmälan ska göras av [ange Part] ifall av en Personuppgiftsincident.

# Kontakt

9.1 Parterna har ett gemensamt ansvar att säkerställa att Registrerades rättigheter tillgodoses enligt Dataskyddsförordningen och annan tillämplig lagstiftning. Parterna är således överens om att en Registrerad kan vända sig till endera Part. För detta Avtal ska [ange Part] vara gemensam kontaktpunkt för de Registrerade och tillsynsmyndigheten.

9.2 Parterna ska utan dröjsmål underrätta den andra Parten om kontakt med de Registrerade som är av betydelse för Behandlingen av Personuppgifter.

9.3 Parterna är överens om att, på begäran av endera Part, bistå varandra med hantering av en Registrerads begäran om att tillvarata sina rättigheter enligt Dataskyddsförordningen. Stöd ska tillhandahållas utan onödigt dröjsmål.

9.4 Parterna ska utan dröjsmål underrätta den andra Parten om Part upptäcker att särskild reglering om Personuppgiftsbehandlingen saknas.

9.5 Kontaktperson för respektive Part samt respektive Parts Dataskyddsombud är:

 Kontaktperson vid UU: [Namn och e-post],

 Dataskyddsombud: dataskyddsombud@uu.se

 Kontaktperson vid […]: [Namn och e-post]

 Dataskyddsombud: [E-post]

# Ansvar

10.1 I fall där Registrerade riktar anspråk avseende ersättning mot någon av Parterna med anledning av materiell eller immateriell skada till följd av överträdelse av Dataskyddsförordningen ska artikel 82 i Dataskyddsförordningen äga tillämpning, enligt vilken det framgår att Parterna är solidariskt ansvariga. Part äger dock rätt att återkräva från annan Part den del av ersättning som motsvarar den andra Partens ansvar för den uppkomna skadan.

10.2 Parterna är överens om att sådana sanktionsavgifter som enligt artikel 83 i Dataskyddsförordningen eller 6 kap. 2 § lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning ska bäras av den Part som påförts sådan avgift.

# Ändringar och tillägg

11.1 Ändringar och tillägg till detta Avtal ska göras skriftligen och undertecknas av Parterna för att vara giltiga.

11.2 Utöver vad som särskilt anges i detta Avtal har ingen av Parterna rätt att helt eller delvis överlåta rättigheterna eller skyldigheterna enligt detta Avtal utan den andra Partens skriftliga medgivande.

# Avtalstid och avslut

12.1 Detta Avtal gäller från det att båda Parter signerat Avtalet och så länge som ett gemensamt personuppgiftsansvar föreligger mellan Parterna

12.2 Såvida annat inte avtalas mellan Parterna eller följer av tillämplig lagstiftning ska vid Avtalets upphörande den Part som inte längre har ansvar för Personuppgifterna radera Personuppgifterna alternativt överföra dessa till den Part som fortsatt anses som ensam ansvarig för Personuppgifterna.

12.3 För det fall att endera Part på grund av lag, förordning, myndighetsföreskrifter eller beslut är skyldigt att behålla Personuppgifter även efter det att detta Avtal har upphört att gälla får dessa Personuppgifter endast användas för det ändamål som framgår av den lag, förordning, myndighets föreskrifter eller beslut som föranleder att Personuppgifterna behålls. Den andra Parten ska i så fall informeras om detta och grunderna härför.

# Tillämplig lag och tvist

13.1 Om inte annat följer av Huvudavtalet ska tvist angående tolkning eller tillämpning av detta Avtal avgöras enligt svensk lag och föras vid allmän svensk domstol. För det fall Parterna är svenska myndigheter ska tvist istället slutligt avgöras av närmast överordnad myndighet eller eljest av den tillämpliga tvistelösningsmekanism inom svenska staten som står till buds.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Detta Avtal upprättats i 2 (två) likalydande exemplar, varav Parterna tagit var sitt.

**Uppsala universitet** **[**Namn]

*Signatur Signatur*

*Namnförtydligande, befattning Namnförtydligande, befattning*

*Ort och datum Ort och datum*

Bilaga 1 – Parternas Personuppgiftsbehandling

Parterna har nedan konkretiserat vad som ingår i Behandlingen enligt Avtalet

1. **Ändamålet med Behandlingen**

Ändamålet med Behandlingen av Personuppgifter är (*varför sker Behandling av Personuppgifter, t.ex. gemensamt forskningsprojekt m.m.).*

1. **Laglig grund för Behandlingen**

Parterna är överens om att den lagliga grunden för Behandlingen är (*t.ex. myndighetsutövning och uppgift av allmänt intresse*).

1. **Kategorier av Registrerade**

De kategorier av Registrerade som berörs är (v*ilka grupper av invånare som Behandlas i systemet, t.ex. kommuninvånare, pensionärer, sparare, elever, anställda inom verksamheten, förtroendevalda, enskilda som mottar tjänst, forskningspersoner m.fl.).*

1. **Vilken typ av Personuppgifter Behandlas**

De Personuppgifter som behandlas är av följande slag: (*t.ex. namn, ip-adress, e-postadress, fastighetsbeteckning, enskild firma m.fl.).*

1. **Känsliga Personuppgifter (i förekommande fall)**

De Känsliga Personuppgifter som Behandlingen rör är: (*t.ex. ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, hälsa och sjukdom, medlemskap i fackförening och Behandling av genetiska och biometriska uppgifter. Vid Behandling av Känsliga Personuppgifter ska det särskilt beaktas att hantering ska ske på särskilt sätt i enlighet med Skatteverkets vägledning för sekretessmarkerade Personuppgifter i offentlig förvaltning.).*

1. **Behandling**

Personuppgifterna kommer att Behandlas på följande sätt *(jfr punkt 3 i Avtalet såsom vem som ansvarar för insamling, registrering, organisering, lagring, bearbetning och spridning eller annat tillhandahållande av uppgifter, sammanställning eller samkörning. Glöm inte att om Känsliga Personuppgifter Behandlas ska de listas här såsom ”Behandling av Känsliga Personuppgifter”).*

1. **Särskilda förutsättningar rörande Behandlingen:**

(*Ange om det finns något särskilt som Parterna ska beakta vid Behandling av Personuppgifterna.*)

1. **Behandling i tredje land (i förekommande fall)**

(*Ange om Personuppgifter överförs, direkt eller indirekt, till land utanför EU/EES.*)

1. **Avslutsrutiner**

Se punkt 12 i Avtalet.

1. **Information om Personuppgiftsbiträden**

(*Ange eventuella biträden nedan.*)

|  |  |  |
| --- | --- | --- |
| **Namn på Personuppgiftsbiträde** | **Typ av Behandling och skälen för Behandlingen** | **Plats för Behandling samt, när utanför EU/EES, laglig grund för överföring av Personuppgifter** |
|  |  |  |
|  |  |  |

Bilaga 2 – Informationssäkerhet

[Personuppgifterna ska i Behandlingen skyddas av informationssäkerhetsmässiga åtgärder som säkerställer en relevant säkerhetsnivå med utgångspunkt från informationens känslighet.

Vid frågor avseende utformningen av Bilaga 2, vänligen kontakta säkerhetsavdelningen, enheten för informationssäkerhet.]

Parterna har genomfört informationsklassificering och en analys baserad på informationssäkerhetsmässiga krav enligt svensk och internationell standard SS-ISO/IEC 27001.

Parterna garanterar att

* Informationssäkerhetsarbete bedrivs i enlighet med ISO/IEC 27001 eller motsvarande inom detta område.
* Utveckling av Parternas informationssystem/IT-tjänster genomförs med hänsyn till informations­säkerhet, det vill säga krav på konfidentialitet, riktighet och tillgänglighet.
* Grundläggande för Parternas hantering av informationssäkerhet är: åtkomstbegränsning, riktighet, spårbarhet och tillgänglighet.
* Skalskydd till Parternas lokaler finns i form av lås och larm. Procedurer finns för tilldelning respektive hantering av utrustning och behörighet och ses över regelbundet.
* Skyddsmekanismer finns i form av brandvägg.
* Endast behörig personal har tillgång till Parternas IT-miljö.
* Parterna har administrativa rutiner och tekniska åtgärder för att information från olika kunder särskiljs.
* Parterna arbetar efter implementerade ledningssystem för informationssäkerhet, som reglerar uppföljning av IT-säkerhetsincidenter.
* Parterna kommer att anmäla eventuella personuppgiftsincidenter som berör Parternas data i uppdraget enligt erhållen kontaktinformation.